

certificate reload

To configure Secure Socket Layer (SSL) Encryption Support enabled to read the profile security certificate from the file specified in the **servercert** command, use the **certificate reload** command in customer profile configuration mode.

certificate reload

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Profile configuration

Command History	Release	Modification
	12.1(5)T	This command was introduced.

Usage Guidelines There is not a **no** form for this command.
The TN3270 server must be configured for security.

Examples The following example configures the TN3270 server with SSL Encryption Support to read the profile security certificate from the file specified in the **servercert** command:

```
certificate reload
```

Related Commands	Command	Description
	servercert	Specifies the location of the TN3270 server's security certificate in the Flash memory.

channel-protocol

To define a data rate of either 3 MBps or 4.5 MBps for Parallel Channel Interfaces, use the **channel-protocol** command in interface configuration mode. To return to the default rate of 3 MBps, use the **no** form of this command.

channel-protocol [s | s4]

no channel-protocol

Syntax Description

s	(Optional) Specifies a data rate of 3 MBps.
s4	(Optional) Specifies a data rate of 4.5 MBps.

Defaults

If no value is specified, the default data rate for the Parallel Channel Adapter (PCA) and the Parallel Channel Port Adapter (PCPA) is 3 MBps.

Command Modes

Interface configuration

Command History

Release	Modification
10.2	This command was introduced.

Usage Guidelines

This command is valid on Parallel Channel Interfaces.

Examples

The following example specifies a data rate of 4.5 MBps for the interface:

```
channel-protocol s4
```

claw (backup)

To configure a Common Link Access for Workstations (CLAW) device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and configure individual members of a CLAW backup group for the IP Host Backup feature, use the **claw** command in IP host backup configuration mode. To remove the CLAW device, use the **no** form of this command.

```
claw path device-address ip-address host-name device-name host-app device-app [broadcast]
```

```
no claw device-address
```

Syntax Description	
<i>path</i>	Hexadecimal value in the range from 0000 to FFFF. This value specifies the logical channel path and consists of two digits for the physical connection (either on the host or on the ESCON director), one digit for the channel logical address, and one digit for the control unit logical address. If the path is not specified in the input/output configuration program (IOCP), the default value for channel logical address and control unit logical address is 0.
<i>device-address</i>	Hexadecimal value in the range from 00 to FE. This is the unit address associated with the control unit number and path as specified in the host IOCP file. The device address must have an even-numbered value.
<i>ip-address</i>	IP address specified in the HOME statement of the host TCP/IP application configuration file.
<i>host-name</i>	Host name specified in the device statement in the host TCP/IP application configuration file.
<i>device-name</i>	CLAW workstation name specified in the device statement in the host TCP/IP application configuration file.
<i>host-app</i>	Host application name as specified in the host application file. When connected to the IBM TCP host offerings, this value will be tcPIP , which is the constant specified in the host TCP/IP application file. When attached to other applications, this value must match the value hard coded in the host application.
<i>device-app</i>	CLAW workstation application specified in the host TCPIP application. When connected to the IBM TCP host offerings, this value will be tcPIP , which is the constant specified in the host TCP/IP application file. When attached to other applications, this value must match the value hard coded in the host application.
broadcast	(Optional) Enables broadcast processing for this subchannel.

Defaults No default behavior or values

Command Modes IP host backup configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command defines information that is specific to the hardware interface and the IBM channels supported on the interface.

CLAW devices are used to switch IP packets between a mainframe and a channel-attached router.

At most, 128 statements can be configured per interface because each interface is limited to 256 subchannels. Each CLAW device uses a read channel and a write channel. There is also a restriction of 64 unique paths.

A limit of 32 CLAW device configuration commands is recommended.

Duplicate IP addresses are invalid for nonbackup configurations.

Duplicate IP addresses are permitted if they appear within a backup group of only **claw** or **offload** interface configuration commands. All configuration commands in one backup group must specify the **backup** keyword.

You can use the **path** interface configuration command to specify a number of paths that belong to a backup group. In that case, a **claw** IP host backup configuration command is used that needs no *path* variable or **backup** keyword.

Examples

The following examples show two methods for entering the same IP host backup group information. The first group of commands is the long form, using the **claw** interface configuration command. The second group is the shortcut, using the **path** interface configuration command and a **claw** IP host backup configuration command.

Long form:

```
claw c000 00 10.92.10.5 sysa router1 tcpip tcpip
claw c100 00 10.92.10.5 sysa router1 tcpip tcpip
claw c200 00 10.92.10.5 sysa router1 tcpip tcpip
```

Shortcut form:

```
path c000 c100 c200
    claw 00 10.92.10.5 sysa router1 tcpip tcpip
```

Related Commands

Command	Description
claw (primary)	Configures a CLAW device (read and write subchannel) for communication with a mainframe TCP/IP stack in IP datagram mode and also configures individual members of a CLAW backup group for the IP Host Backup feature.
offload (backup)	Configures a backup group of Offload devices.
offload (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.
show extended channel packing names	Displays CLAW packing names and their connection state.

Command	Description
show extended channel packing stats	Displays CLAW packing statistics.
show extended channel statistics	Displays statistical information about subchannels on the physical interface of a CMCC adapter and displays information that is specific to the interface channel devices. The information generally is useful only for diagnostic tasks performed by technical support personnel.
show extended channel subchannel	Displays information about the CMCC adapter physical interfaces and displays information that is specific to the interface channel connection. The information displayed generally is useful only for diagnostic tasks performed by technical support personnel.

claw (primary)

To configure a Common Link Access for Workstations (CLAW) device (read and write subchannel) for communication with a mainframe TCP/IP stack in IP datagram mode and also configure individual members of a CLAW backup group for the IP Host Backup feature, use the **claw** command in interface configuration mode. To remove the CLAW device, use the **no** form of this command.

claw *path device-address ip-address host-name device-name host-app device-app* [**broadcast**] [**backup**]

no **claw** *path device-address*

Syntax Description

<i>path</i>	Hexadecimal value in the range from 0000 to FFFF. This value specifies the logical channel path and consists of two digits for the physical connection (either on the host or on the ESCON director), one digit for the channel logical address, and one digit for the control unit logical address. If the path is not specified in the input/output configuration program (IOCP), the default value for channel logical address and control unit logical address is 0.
<i>device-address</i>	Hexadecimal value in the range from 00 to FE. This is the unit address associated with the control unit number and path as specified in the host IOCP file. The device address must have an even-numbered value.
<i>ip-address</i>	IP address specified in the HOME statement of the host TCP/IP application configuration file.
<i>host-name</i>	Host name specified in the device statement in the host TCP/IP application configuration file.
<i>device-name</i>	CLAW workstation name specified in the device statement in the host TCP/IP application configuration file.
<i>host-app</i>	Host application name as specified in the host application file. When connected to the IBM TCP host offerings, or if the CLAW packing feature is not enabled on the mainframe TCPIP stack, this value will be tcpip , which is the constant specified in the host TCP/IP application file. When attached to other applications, this value must match the value hard coded in the host application. The value packed can be used for the <i>host-app</i> argument to enable the CLAW packing feature.
<i>device-app</i>	CLAW workstation application specified in the host TCPIP application. If connected to the IBM TCP host offerings, or if the CLAW packing feature is not enabled on the mainframe TCPIP stack, this value will be tcpip , which is the constant specified in the host TCP/IP application file. When attached to other applications, this value must match the value hard coded in the host application. The value packed can be used for the <i>device-app</i> argument to enable the CLAW packing feature.
broadcast	(Optional) Enables broadcast processing for this subchannel.
backup	(Optional) Enables this CLAW connection to be used as part of a backup group of CLAW connections for the specified IP address.

Defaults

No default behavior or values

Command Modes Interface configuration

Command History	Release	Modification
	10.2	This command was introduced.
	12.0	The following options were added: <ul style="list-style-type: none"> • backup • packed

Usage Guidelines This command defines information that is specific to the hardware interface and the IBM channels supported on the interface. When used with the **path** command, the **claw** command provides a quick way to configure a CLAW backup group.

CLAW devices are used to switch IP packets between a mainframe and a channel-attached router.

At most, 128 statements can be configured per interface because each interface is limited to 256 subchannels. Each CLAW device uses a read channel and a write channel. There is also a restriction of 64 unique paths.

A limit of 32 CLAW device configuration commands is recommended.

Duplicate IP addresses are invalid for nonbackup configurations.

Duplicate IP addresses are permitted if they appear within a backup group of only **claw** or **offload** interface configuration commands. All configuration commands in one backup group must specify the **backup** keyword.

You can use the **path** interface configuration command to specify a number of paths that belong to a backup group. In that case, a **claw** IP host backup configuration command is used that needs no *path* variable or **backup** keyword. You can use the **packed** value as an optional keyword for the *host-app* and *device-app* arguments.

Examples The following example shows how to enable IBM channel attach routing on channel interface 3/0, which is supporting an ESCON direct connection to the mainframe:

```
interface channel 3/0
ip address 172.18.4.49 255.255.255.248
claw c020 F4 172.18.4.52 HOSTB RTRA TCPIP TCPIP
```

The following example shows how to enable CLAW packing:

```
interface Channel 3/0
ip address 172.18.4.49 255.255.255.248
claw c010 F2 172.18.4.50 HOSTA RTRA PACKED PACKED
```

The following example shows how an IP host backup group is specified using the **backup** keyword:

```
interface Channel3/0
no ip address
no keepalive
no shutdown
claw 0100 C0 10.30.1.2 CISCOVM EVAL TCPIP TCPIP backup
```

```
claw 0110 C0 10.30.1.2 CISCOVM EVAL TCPIP TCPIP backup
claw 0120 C0 10.30.1.2 CISCOVM EVAL TCPIP TCPIP backup
claw 0110 C2 10.30.1.3 CISCOVM EVAL TCPIP TCPIP
```

Related Commands

Command	Description
claw (backup)	Configures a CLAW device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of a CLAW backup group for the IP Host Backup feature.
offload (backup)	Configures a backup group of Offload devices.
offload (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.
show extended channel packing names	Displays CLAW packing names and their connection state.
show extended channel packing stats	Displays CLAW packing statistics.
show extended channel statistics	Displays statistical information about subchannels on the physical interface of a CMCC adapter and displays information that is specific to the interface channel devices. The information generally is useful only for diagnostic tasks performed by technical support personnel.
show extended channel subchannel	Displays information about the CMCC adapter physical interfaces and displays information that is specific to the interface channel connection. The information displayed generally is useful only for diagnostic tasks performed by technical support personnel.

clear alps circuits

To remove configured Airline Product Set (ALPS) circuits, use the **clear alps circuits** command in user EXEC or privileged EXEC mode.

```
clear alps circuits [ipaddr address | name string]
```

Syntax Description

ipaddr <i>address</i>	(Optional) Clear ALPS circuits for peer with specified IP address.
name <i>string</i>	(Optional) Clear ALPS circuits for peer with specified name.

Defaults

If no IP address or name is specified, the command clears all ALPS circuits.

Command Modes

EXEC

Command History

Release	Modification
11.3(6)T	This command was introduced.

Examples

The following example clears the ALPS circuit named CKT1:

```
Router# clear alps circuits name CKT1
```

Related Commands

Command	Description
alps auto-reset	Automatically resets a nonresponsive ALC ASCU in the DOWN state.
show alps circuits	Displays the status of the ALPS circuits.

clear alps counters

To clear all counters relevant to the ALPS feature, use the **clear alps counters** command in user EXEC or privileged EXEC mode.

clear alps counters

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	11.3(6)T	This command was introduced.

Examples The following example clears all counters for the ALPS feature:

```
Router# clear alps counters
```

Related Commands	Command	Description
	encapsulation uts	Specifies that the P1024C UTS protocol will be used on the serial interface.
	show alps circuits	Displays the status of the ALPS circuits.
	show alps peers	Displays the status of the ALPS partner peers.

clear dbconn connection

To break a client connection to DATABASE2 (DB2), use the **clear dbconn connection** command in privileged EXEC configuration mode, specifying the ID of the connection you want to terminate.

```
clear dbconn connection connection-id
```

Syntax Description	<i>connection-id</i>	Identification number for client connection to DB2.
---------------------------	----------------------	---

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	11.3(2)T	
12.0(5)XN		This command was moved from the Cisco Database Connection (CDBC) feature to the Cisco Transaction Connection (CTRC) feature.
12.0(7)T		This command was integrated into Cisco IOS Release 12.0T.

Examples The following example shows the client connection 786A7C being cleared:

```
Router# clear dbconn connection 786A7C

Connection 786A7C cleared
```

Related Commands	Command	Description
		show dbconn connection

clear dbconn statistic

To clear a specific statistic or all Cisco Transaction Connection (CTRC) statistics concerning communications with DB2, use the **clear dbconn statistic** command in privileged EXEC configuration mode.

```
clear dbconn statistic {chains | clientturnaround | connectionsdown | connectionsup | every |
  hostreceived | hostresponse | hostsent | maxconnections}
```

Syntax Description		
	chains	Clears the number of command chains created between CTRC and DATABASE2 (DB2).
	clientturnaround	Clears statistics for the average time from receiving a DB2 client communication to sending that client a response.
	connectionsdown	Clears statistics for the number of connections down between CTRC and DB2.
	connectionsup	Clears statistics for number of connections created between CTRC and DB2.
	every	Clears the complete statistics dump between CTRC and DB2.
	hostreceived	Clears statistics for the number of bytes received from DB2 hosts.
	hostresponse	Clears statistics for the average DB2 host response time.
	hostsent	Clears statistics for the number of bytes sent to DB2 hosts.
	maxconnections	Clears statistics for the maximum number of concurrent connections to Customer Information Control System (CICS) clients.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(5)XN	This command was introduced.
	12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.

Examples The following example clears the stored statistics for the number of bytes the current router has received from DB2 hosts:

```
Router# clear dbconn statistic hostreceived
```

Related Commands	Command	Description
	show dbconn statistic	Displays all CTRC statistics concerning communications with DB2.

clear dlsw circuit

To cause all data-link switching plus (DLSw+) circuits to be closed, use the **clear dlsw circuit** command in privileged EXEC configuration mode.

```
clear dlsw circuit [circuit-id]
```

Syntax Description	<i>circuit-id</i>	Circuit ID for a specific remote circuit. The valid range is from 0 to 4294967295.
---------------------------	-------------------	--

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	11.2 F	This command was introduced.

Usage Guidelines	A user can specify a circuit ID of a specific circuit to clear rather than clearing all circuits.
-------------------------	---



This command also drops the associated Logical Link Control, type 2 (LLC2) session. The command usage should be used with caution and under the advice of a Cisco engineer.

Examples	The following example closes all DLSw+ circuits:
-----------------	--

```
Router# clear dlsw circuit
```

clear dlsw history

To clear all currently inactive circuits from the DLSw+ circuit history, use the **clear dlsw history** privileged EXEC command.

clear dlsw history

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1	This command was introduced.

Examples The following example clears all inactive circuits from the DLSW+ circuit history:

```
clear dlsw history
```

clear dlsw local-circuit

To cause all locally-switched DLSw+ circuits to be closed, use the **clear dlsw local-circuit** privileged EXEC command.

```
clear dlsw local-circuit [circuit-id]
```

Syntax Description	<i>circuit-id</i> Circuit ID for a specific remote circuit. The valid range is 0 to 4294967295.
---------------------------	---

Defaults	No default behavior or values.
-----------------	--------------------------------

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	12.1	This command was introduced.

Usage Guidelines	A user can specify a circuit ID of a specific circuit to clear rather than clearing all local-switched circuits.
-------------------------	--



Caution

This command also drops the associated LLC2 session. The command usage should be used with caution and under the advice of a Cisco engineer.
--

Examples	The following example closes the locally-switched DLSw+ circuit with ID number 100:
-----------------	---

```
clear dlsw local-circuit 100
```

clear dlsw reachability

To remove all entries from the data-link switching plus (DLSw+) reachability cache, use the **clear dlsw reachability** command in privileged EXEC configuration mode.

clear dlsw reachability

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	11.2 F	This command was introduced.

Usage Guidelines This command does not affect existing sessions.

Examples The following example removes all entries from the DLSw+ reachability cache:

```
Router# clear dlsw reachability
```

clear dlsw statistics

To reset to zero the number of frames that have been processed in the local, remote, and group cache, use the **clear dlsw statistics** command in privileged EXEC configuration mode.

clear dlsw statistics

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	11.2 F	This command was introduced.

Examples The following example resets to zero the number of frames in the local, remote, and group cache:

```
Router# clear dlsw statistics
```

clear dlsw transparent

To clear DLSw+ transparent local MAC entries, use the **clear dlsw transparent** privileged EXEC command.

clear dlsw transparent

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1	This command was introduced.

Usage Guidelines This command is designed to be used in networks that employ DLSw+ Ethernet redundancy without transparent mappings.

Examples The following example clears DLSw+ transparent local MAC entries:

```
clear dlsw transparent
```

clear extended counters

To clear the extended interface counters associated with Cisco Mainframe Channel Connection (CMCC) features, use the **clear extended counters** command in user EXEC or privileged EXEC mode.

```
clear extended counters [channel slot/port [csna | icmp-stack | ip-stack | llc2 | statistics |
tcp-connections | tcp-stack | tg | tn3270-server | udp-stack]]
```

Syntax Description		
channel	(Optional)	Specifies a channel interface.
<i>slot</i>	(Optional)	Slot number.
<i>port</i>	(Optional)	Port number.
csna	(Optional)	Clears Cisco Systems Network Architecture (CSNA) feature counters.
icmp-stack	(Optional)	Clears Internet Control Message Protocol (ICMP) stack counters.
ip-stack	(Optional)	Clears IP stack counters.
llc2	(Optional)	Clears Logical Link Control, type 2 (LLC2) counters.
statistics	(Optional)	Clears subchannel statistic counters.
tcp-connections	(Optional)	Clears TCP connection counters.
tcp-stack	(Optional)	Clears TCP stack counters.
tg	(Optional)	Clears Transmission Group (TG) counters.
tn3270-server	(Optional)	Clears TN3270 server counters.
udp-stack	(Optional)	Clears User Datagram Protocol (UDP) stack counters.

Command Modes	
	User EXEC Privileged EXEC

Command History	Release	Modification
	11.3	This command was introduced.

Usage Guidelines	
	This command is valid on both the physical and virtual channel interfaces. To clear counters for a selected CMCC feature, you must specify the channel interface on which the feature is configured or running.
	Counters displayed using the show extended channel EXEC command are cleared using this command.
	Entering any form of this command will prompt the user for a confirmation before clearing any counters. A "CLEAR-5-EXT_COUNT" message is displayed to indicate completion of the command.
	These counters will be cleared in the show commands and remain uncleared when obtained through the Simple Network Management Protocol (SNMP) interface.

Examples

The following example shows how to clear the extended interface counters:

```
Router# clear extended counters
```

Related Commands

Command	Description
show extended channel csna	Displays information about the CSNA subchannels configured on the specified CMCC interface.
show extended channel icmp-stack	Displays information about the ICMP stack running on the CMCC channel interfaces.
show extended channel ip-stack	Displays information about the IP stack running on CMCC channel interfaces.
show extended channel lan	Displays the internal LANs and adapters configured on a CMCC adapter.
show extended channel llc2	Displays information about the LLC2 sessions running on the CMCC adapter interfaces.
show extended channel statistics	Displays statistical information about subchannels on the physical interface of a CMCC adapter and displays information that is specific to the interface channel devices. The information generally is useful only for diagnostic tasks performed by technical support personnel.
show extended channel tcp-connections	Displays information about the TCP sockets on a channel interface.
show extended channel tcp-stack	Displays information about the TCP stack running on CMCC adapter interfaces.
show extended channel udp-listeners	Displays information about the UDP listener sockets running on the CMCC adapter interfaces.
show extended channel udp-stack	Displays information about the UDP stack running on the CMCC adapter interfaces.

clear ncia circuit

To drop a specified native client interface architecture (NCIA) circuit, use the **clear ncia circuit** command in privileged EXEC configuration mode.

```
clear ncia circuit [id-number]
```

Syntax Description

<i>id-number</i>	(Optional) Number assigned to identify the circuit. If no circuit ID number is specified, the command drops all circuits.
------------------	---

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

If no circuit ID number is specified, the command drops all circuits.

Examples

The following example clears the active NCIA circuit identified as 791F8C:

```
Router# clear ncia circuit 791F8C
```

Related Commands

Command	Description
show ncia circuits	Displays the state of all circuits involving this MAC address as a source and destination.

clear ncia client registered

To release the control block of a specified registered client after terminating the active connection to it, use the **clear ncia client registered** command in privileged EXEC configuration mode.

clear ncia client registered [*ip-address*]

Syntax Description	<i>ip-address</i>	(Optional) IP address of the registered client. If no IP address is specified in the command, the command releases the control blocks of all registered clients after terminating any active connections to them.
---------------------------	-------------------	---

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines	If no IP address is specified in the command, the command releases the control blocks of all registered clients after terminating any active connections to them.
-------------------------	---

Examples	The following example terminates the active connection to the registered client identified by the IP address 10.2.20.126 and releases its control block:
-----------------	--

```
Router# clear ncia client registered 10.2.20.126
```

Related Commands	Command	Description
	show ncia client	Displays the status of the NCIA client.

clear ncia client

To terminate a specified active client connection, use the **clear ncia client** command in privileged EXEC configuration mode.

```
clear ncia client [ip-address]
```

Syntax Description

<i>ip-address</i>	(Optional) IP address of the client. If no IP address is specified in the command, the command terminates all active client connections.
-------------------	--

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

If no IP address is specified in the command, the command terminates all active client connections.

Examples

The following example terminates the active connection to the client identified by the IP address 10.2.20.126:

```
Router# clear ncia client 10.2.20.126
```

Related Commands

Command	Description
show ncia client	Displays the status of the NCIA client.

clear txconn connection

To clear a Cisco Transaction Connection (CTRC) connection to a Customer Information Control System (CICS) client and all associated transactions, use the **clear txconn connection** command in privileged EXEC configuration mode.

```
clear txconn connection connection-id
```

Syntax Description

<i>connection-id</i>	CICS connection identification number.
----------------------	--

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T12.0(7)T

Examples

The following example clears the specified CICS client connection number 62146088 and all its transactions:

```
Router# clear txconn connection 62146088
% Connection 62146088 cleared
```

Related Commands

Command	Description
clear txconn transaction	Terminates a specified CICS transaction.
show txconn connection	Displays a list of all of the CTRC connections of the router to CICS clients.

clear txconn statistic

To clear a specific statistic or all Cisco Transaction Connection (CTRC) statistics concerning communications with Customer Information Control System (CICS), use the **clear txconn statistic** command in privileged EXEC configuration mode.

```
clear txconn statistic {allocatetime | clientreceived | clientsent | clientturnaround | every |
  hostreceived | hostresponse | hostsent | maxconnections | maxtransactions |
  totalconnections | totaltransactions}
```

Syntax Description		
	allocatetime	Clears statistics for the average time spent waiting for Advanced Program-to-Program Communication (APPC) allocate operation to complete.
	clientreceived	Clears statistics for the number of bytes received from CICS clients.
	clientsent	Clears statistics for the number of bytes sent to CICS clients.
	clientturnaround	Clears statistics for the average time from receiving a CICS client communication to sending that client a response.
	every	Clears every statistic concerning the current router's CTRC communications with CICS.
	hostreceived	Clears statistics for the number of bytes received from CICS hosts.
	hostresponse	Clears statistics for the average CICS host response time.
	hostsent	Clears statistics for the number of bytes sent to CICS hosts.
	maxconnections	Clears statistics for the maximum number of concurrent connections to CICS clients.
	maxtransactions	Clears statistics for the maximum number of concurrent transactions with CICS hosts.
	totalconnections	Clears statistics for the total number of connections to CICS clients.
	totaltransactions	Clears statistics for the total number of CICS transactions processed.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(5)XN	This command was introduced.
	12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Examples The following example clears the stored statistics for the number of bytes the current router has received from CICS clients:

```
Router# clear txconn statistic clientreceived
```

Related Commands

Command	Description
show txconn statistic	Displays information about the CTRC communications of the current router with CICS.

clear txconn transaction

To terminate a specified Customer Information Control System (CICS) transaction, use the **clear txconn transaction** command in privileged EXEC configuration mode. This command terminates the conversation with the host and returns DEALLOC_ABEND_PROG to the client.

clear txconn transaction *transaction-id*

Syntax Description	<i>transaction-id</i>	ID of the CICS transaction to be cleared.
---------------------------	-----------------------	---

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	12.0(5)XN	This command was introduced.
	12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Examples The following example clears the CICS transaction number 621FC8E0:

```
Router# clear txconn transaction 621FC8E0
% Transaction 621FC8E0 cleared
```

Related Commands	Command	Description
	clear txconn connection	Clears a CTRC connection to a CICS client and all associated transactions.
	show txconn transaction	Displays a list of all the CTRC transactions of the current router with CICS, transactions of a specified CTRC server, or transactions of a specified CICS client connection.

client ip

To add an IP subnet to a client subnet response-time group, use the **client ip** command in response-time configuration mode. To remove an IP subnet from a client subnet response-time group, use the **no** form of this command.

client ip *ip-address* [*ip-mask*]

no client ip *ip-address* [*ip-mask*]

Syntax Description

<i>ip-address</i>	IP subnet being added to the response-time group.
<i>ip-mask</i>	(Optional) Mask applied to a client IP address to determine the client's membership in a client subnet group. When the mask is applied to a connecting client's IP address and the resulting address is equal to the defined IP address, the client becomes a member of the client group. The default mask is 255.255.255.255.

Defaults

The default mask is 255.255.255.255.

Command Modes

Response-time configuration

Command History

Release	Modification
11.2(18)BC	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0 T.

Examples

The following example adds an IP subnet to a client subnet response-time group:

```
tn3270-server
response-time group acctg
client ip 10.1.2.3 255.0.0.0
```

Related Commands

Command	Description
response-time group	Configures a client subnet group for response-time measurements.
show extended channel tn3270-server response-time application	Displays information about application response-time client groups.
show extended channel tn3270-server response-time global	Displays information about the global response-time client group.
show extended channel tn3270-server response-time link	Displays information about host link response-time client groups.
show extended channel tn3270-server response-time listen-point	Displays information about listen point response-time client groups.

Command	Description
show extended channel tn3270-server response-time subnet	Displays information about Subnet response-time client groups.
tn3270-server	Starts the TN3270 server on a CMCC adapter and enters TN3270 server configuration mode.

client ip lu

To define a specific logical unit (LU) or range of LUs to a client at the IP address or subnet, use the **client ip lu** command in TN3270 PU configuration mode. To cancel this definition, use the **no** form of this command.

```
client [printer] ip ip-address [ip-mask] lu first-locaddr [last-locaddr]
```

```
no client [printer] ip ip-address [ip-mask] lu first-locaddr [last-locaddr]
```

Syntax Description

printer	(Optional) Specifies that a client connection from the nailed IP addresses will be nailed to one of the specified LUs only if the client session negotiates a model type of 328x, where <i>x</i> is any alphanumeric character. Moreover, it ensures that a printer matching the IP address condition can used only an LU nailed as a printer LU. If the printer keyword is not specified for any client statement that has this IP address set, all model types can use this range of LUs.
<i>ip-address</i>	Specifies the remote client IP address.
<i>ip-mask</i>	(Optional) The mask applied to the remote device address. Multiple client IP addresses in the same subnet can be nailed to the same range of local address.
<i>first-locaddr</i>	Defines a single local address to nail.
<i>last-locaddr</i>	(Optional) Defines the end range of inclusive local address to be nailed from <i>first-locaddr</i> to <i>last-locaddr</i> .

Defaults

No LUs are nailed. They are all available to any client.

Command Modes

TN3270 PU configuration mode

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

This command is valid only on the virtual channel interface. Multiple statements can be configured for one IP address or nail type either on one PU or multiple PUs. But each LU can appear in only one **client** statement.

A client with a nailed IP address can request one of the nailed LUs via the TN3270 device name. If the requested LU is not available then the connection is rejected.

A client with a nailed IP address cannot request an LU outside the range of nailed LUs for its type (screen or printer).

A client with a nonnailed IP address cannot request an LU that is configured as nailed.

The command will be rejected if some of the local address are already nailed. If the local address are in use by other remote clients, the nailing statement will take effect only when the local address is made available.

To cancel the definition, the **no client** form of the command must be entered exactly as the **client** command was originally configured. If a range of local address was specified, to cancel this definition the whole range of local address must be specified. There is no way to cancel only one local address if a whole range of local address was configured.

Examples

In the following example, local address from 1 to 50 are reserved for remote devices in the 10.69.176.0 subnet:

```
interface channel 2/2
tn3270-server
pu BAGE4
client ip 10.69.176.28 255.255.255.0 lu 1 50
```

In the following example, local address 1 to 40 are reserved for screen devices in the 10.69.176.0 subnet, and 41 to 50 are reserved for printers in that subnet:

```
interface channel 2/2
tn3270-server
pu BAGE4
client ip 10.69.176.28 255.255.255.0 lu 1 40
client printer ip 10.69.176.28 255.255.255.0 lu 41 50
```

In the following example, an attempt to cancel a definition is rejected because it does not specify the full range of local address and the second attempt fails to specify the correct nail type:

```
interface channel 2/2
tn3270-server
pu BAGE4
client printer ip 10.69.176.50 255.255.255.0 lu 1 100
no client printer ip 10.69.176.50 255.255.255.0 lu 1
%Invalid LU range specified
no client ip 10.69.176.50 255.255.255.0 lu 1 100
%client ip 10.69.176.50 nail type not matched with configured nail type printer
```

Related Commands

Command	Description
pu (DLUR)	Creates a PU entity that has no direct link to a host and enters DLUR PU configuration mode.

client ip pool

To nail clients to pools, use the **client ip pool** command in listen-point configuration mode. To remove clients from pools, use the **no** form of this command.

client ip *ip-address* [*ip-mask*] **pool** *poolname*

no client ip *ip-address* [*ip-mask*] **pool** *poolname*

Syntax Description

<i>ip-address</i>	Remote client IP address.
<i>ip-mask</i>	(Optional) Mask applied to the remote device address. The mask is part of the matching function that determines whether a client is governed by the nailing statement. The default is 255.255.255.255. Multiple client IP addresses in the same subnet can be nailed to the same range of local address.
<i>poolname</i>	Specifies a unique pool name. The pool name cannot exceed eight characters in length.

Defaults

No clients are nailed to pools.

Command Modes

Listen-point configuration

Command History

Release	Modification
11.2(18)BC	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.

Usage Guidelines

If the pool is configured while logical unit (LU)s are in use, existing clients are allowed to complete their sessions. A pool name can be identical to an LU name. When assigning an LU, the TN3270 server searches the LU name space first for specific requests, such as connections that specify a device name on CONNECT or LU name in the terminal type negotiation. The request is assumed to be directed to the specific LU rather than to the pool. Make sure the name spaces do not clash.

Examples

The following is an example of the **client ip pool** command that nails the client at IP address 10.1.2.3 with an IP mask of 255.255.255.0 to the pool named POOL-1:

```
tn3270-server
pool POOL-1 cluster layout 10s1p
listen-point 172.18.4.18
client ip 10.1.2.3 255.255.255.0 pool POOL-1
```

Related Commands	Command	Description
	listen-point	Defines an IP address for the TN3270 server.
	pool	Defines pool names for the TN3270 server and specifies the number of screens and printers in each logical cluster.
	pu (listen-point)	Creates a PU entity that has a direct link to a host and enters listen-point PU configuration mode.
	pu dlur (listen-point)	Creates a PU entity that has no direct link to a host and enters listen-point PU configuration mode.
	tn3270-server	Starts the TN3270 server on a CMCC adapter and enters TN3270 server configuration mode.

client lu maximum

To limit the number of logical unit (LU) sessions that can be established for each client IP address or IP subnet address, use the **client lu maximum** TN3270 server configuration command. To remove a single LU limit associated with a particular IP address, use the **no** form of this command.

client [*ip-address* [*ip-mask*]] **lu maximum** *number*

no client [*ip-address* [*ip-mask*]]

Syntax Description

<i>ip-address</i>	(Optional) IP address of the client. The value for the <i>ip</i> argument is optional when setting the maximum number of LU sessions. If no IP address is specified, then the limit is applied to all clients.
<i>ip-mask</i>	(Optional) IP network mask for the client. The default is 255.255.255.255.
<i>number</i>	(Optional) Maximum number of LU sessions. The allowed value is from 0 to 65535.

Defaults

The default is that there is no limit on the number of concurrent sessions from one client IP address. The default value for the *ip-mask* argument is 255.255.255.255. In the **no** form of this command, the default value for the *number* argument is 65535.

Command Modes

TN3270 server configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command is valid only on the virtual channel interface. An instance of the **client** (lu limit) command on a given tn3270-server is uniquely identified by the *ip-mask* and the logical AND of the *ip-address* with that mask. For example, if the command is entered as the following:

```
client 10.1.1.62 255.255.255.192 lu maximum 2
```

Then it will be stored (and subsequently displayed by **write term**) as:

```
client 10.1.1.0 255.255.255.192 lu maximum 2
```

The maximum specified on the command can be changed by reissuing the command with the new value. It is not necessary to remove the command first.

When you use the **no client** command, only the corresponding **client lu maximum** statement is removed, as identified by the IP address and IP address mask combination. You cannot use the **no client** command to specify an unlimited number of LU sessions. The **lu maximum** keyword is optional in the **no** form of the command.

For example, if a service bureau has 8000 clients and each client IP address is limited to four LU sessions, you will never need more than 32000 concurrent LU definitions even when the service is running at 100 percent capacity.

Examples

The following example limits all clients to a maximum of two LU sessions:

```
client lu maximum 2
```

The following example limits a client at IP address 10.1.1.28 to a maximum of three LU sessions:

```
client 10.1.1.28 lu maximum 3
```

The LU limit can be applied to different subnets as shown in the following example. The most exact match to the client IP address is chosen. Clients with IP addresses that reside in the subnet 10.1.1.64 (those with IP addresses in the range from 10.1.1.64 through 10.1.1.127) are limited to a maximum of five LU sessions while other clients with IP addresses in the subnet 10.1.1.0 are limited to a maximum of four LU sessions.

```
client 10.1.1.0 255.255.255.0 lu maximum 4
client 10.1.1.64 255.255.255.192 lu maximum 5
```

The following example prevents an LU session for the client at IP address 10.1.1.28:

```
client 10.1.1.28 lu maximum 0
```

Related Commands

Command	Description
maximum-lus	Limits the number of LU control blocks that will be allocated for TN3270 server use.

client pool

To nail clients to pools, use the **client pool** command in listen-point configuration mode. To remove clients from pools, use the **no** form of this command.

client {[**ip** *ip-address* [*ip-mask*]] | [**name** *DNS-name* [*DNS-domain-identifier*]] | [**domain-name** *DNS-domain*] | [**domain-id** *DNS-domain-identifier*]} **pool** *poolname*

no client {[**ip** *ip-address* [*ip-mask*]] | [**name** *DNS-name* [*DNS-domain-identifier*]] | [**domain-name** *DNS-domain*] | [**domain-id** *DNS-domain-identifier*]} **pool** *poolname*

Syntax Description		
ip <i>ip-address</i>		Remote client IP address.
<i>ip-mask</i>		(Optional) Mask applied to the remote device address. The mask is part of the matching function that determines whether a client is governed by the nailing statement. The default is 255.255.255.255. Multiple client IP addresses in the same subnet can be nailed to the same pool.
name <i>DNS-name</i>		(Optional) Alphanumeric string that specifies a client machine name. The string can contain up to 24 characters. If a valid <i>DNS-domain-identifier</i> is not present, this name must be fully qualified. If this name is not fully qualified, any dot that forms the boundary between the Domain Name System (DNS) name and the DNS domain must be included here if it is not already present in the DNS domain.
<i>DNS-domain-identifier</i>		(Optional) A numeric identifier that specifies a domain name. The valid value range is from 1 to 255. Each domain-id command statement can have only one <i>DNS-domain-identifier</i> value.
domain-name <i>DNS-domain</i>		(Optional) Alphanumeric string that specifies a domain name suffix, including all dots (.) but not delimited by dots. The string can contain up to 80 characters. All dots must be included when the string is appended to a configured DNS-name. If the DNS-domain starts with a dot, then the dot must be included if it is not already at the end of the DNS-name.
domain-id <i>DNS-domain-identifier</i>		(Optional) Numeric identifier that specifies that a domain name suffix will be appended to the name configured in the domain-id command. The valid value range is from 1 to 255. Each domain-id command statement can have only one <i>DNS-domain-identifier</i> value. The domain id is originally specified in the domain-id command.
<i>poolname</i>		Specifies a unique pool name. The pool name cannot exceed eight characters in length.

Defaults No default behavior or values

Command Modes Listen-point configuration

Command History

Release	Modification
11.2(18)BC	This command was introduced.
12.0(5)T	This command was integrated in Cisco IOS Release 12.0 T.
12.1(5)T	This command was modified to include the name , domain-name , and domain-id keywords. The name of the command was changed from client ip pool to client pool .

Usage Guidelines

If the pool is configured while logical units (LU)s are in use, existing clients are allowed to complete their sessions. A pool name can be identical to an LU name. When assigning an LU, the TN3270 server searches the LU name space first for specific requests, such as connections that specify a device name on CONNECT or LU name in the terminal type negotiation. The request is assumed to be directed to the specific LU rather than to the pool. Make sure the LU names do not conflict.

Examples**Nailing Clients to Pools by IP Address**

The following is an example of the **client pool** command with the **ip** keyword configured. The command nails the client at IP address 10.1.2.3 with an IP mask of 255.255.255.0 to the pool named POOL-1:

```
tn3270-server
 pool POOL-1 cluster layout 10slp
 listen-point 172.18.4.18
 client ip 10.1.2.3 255.255.255.0 pool POOL-1
```

Nailing Clients to Pools by Device Name

The following is an example of the **client pool** command with the **name** keyword configured. The command nails the client at device name user1.cisco.com to the pool named POOL-2:

```
tn3270-server
 pool POOL-2 cluster layout 4slp
 listen-point 172.18.5.168
 pu T240CA 91922363 token-adapter 31 12 rmac 4000.4000.0001
 allocate lu 1 pool POOL-2 clusters 1
 client name user1.cisco.com pool POOL-2
```

Nailing Clients to Pools by Device Name Using a Domain ID

The following is an example of the **client pool** command with the **name** keyword and the optional *DNS-domain-identifier* argument configured. The command nails the client at device name lucy-isdn49.cisco.com to the pool named POOL-2:

```
tn3270-server
 domain-id 23 .cisco.com
 pool POOL-2 cluster layout 4slp
 listen-point 172.18.5.168
 pu T240CA 91922363 token-adapter 31 12 rmac 4000.4000.0001
 allocate lu 1 pool POOL-2 clusters 1
 client name lucy-isdn49 23 pool POOL-2
```

Nailing Clients to Pools by Domain Name

The following is an example of the **client pool** command with the **domain-name** keyword configured. The command nails any client at domain name cisco.com to the pool named POOL-2:

```
tn3270-server
 pool POOL-2 cluster layout 4slp
 listen-point 172.18.5.168
```

```

pu T240CA 91922363 token-adapter 31 12 rmac 4000.4000.0001
  allocate lu 1 pool POOL-2 clusters 1
client domain-name .cisco.com pool POOL-2

```

Nailing Clients to Pools by Domain Name Using a Domain ID

The following is an example of the **client pool** command with the **domain-id** keyword configured. The command nails any client at domain name cisco.com to the pool named POOL-2:

```

tn3270-server
domain-id 23 .cisco.com
pool POOL-2 cluster layout 4s1p
listen-point 172.18.5.168
  pu T240CA 91922363 token-adapter 31 12 rmac 4000.4000.0001
    allocate lu 1 pool POOL-2 clusters 1
client domain-id 23 pool POOL-2

```

Related Commands

Command	Description
listen-point	Defines an IP address for the TN3270 server.
pool	Defines pool names for the TN3270 server and specifies the number of screens and printers in each logical cluster.
pu dlur (listen-point)	Creates a PU entity that has no direct link to a host and enters listen-point PU configuration mode.
pu (listen-point)	Creates a PU entity that has a direct link to a host and enters listen-point PU configuration mode.
tn3270-server	Starts the TN3270 server on a CMCC adapter and enters TN3270 server configuration mode.
domain-id	Specifies a domain name suffix that the TN3270 server appends to a configured machine name to form a fully-qualified name when configuring inverse DNS nailing.

cmPC

To configure a Cisco Multipath Channel (CMPC or CMPC+) read subchannel and a CMPC (or CMPC+) write subchannel, use the **cmPC** command in interface configuration mode. To remove a subchannel definition and to deactivate the transmission group, use the **no** form of this command.

```
cmPC path device tg-name {read | write}
```

```
no cmPC path device
```

Syntax Description

<i>path</i>	Hexadecimal value in the range from 0000 to FFFF. This value specifies the logical channel path and consists of two digits for the physical connection (either on the host or on the ESCON director), one digit for the channel logical address, and one digit for the control unit logical address. If the path is not specified in the input/output configuration program (IOCP), the default value for channel logical address and control unit logical address is 0.
<i>device</i>	Hexadecimal value in the range from 00 to FF. This is the unit address associated with the control unit number and path as specified in the host IOCP file.
<i>tg-name</i>	Name of the CMPC or CMPC+ Transmission Group (TG). The maximum length of the name is eight characters.
read	Same read value as specified in the Transport Resource List (TRL) major node.
write	Same write value as specified in the TRL major node.

Defaults

No default is specified.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(3)T	Support was added for the CMPC+ feature.

Usage Guidelines

Each **cmPC** configuration command in a given CMPC or CMPC+ TG specifies the same TG name. The corresponding **tg** command specifies the same TG name. Together, the **cmPC** and **tg** commands make up the TG specification.

The **cmPC** command defines the read/write subchannel addresses that CMPC or CMPC+ uses to connect to the host. The command corresponds to the definitions in the TRL major node on the host. Configure the **cmPC** command on a Cisco Mainframe Channel Connection (CMCC) adapter physical interface. Configure one read subchannel and one write subchannel. If CMPC or CMPC+ is configured on a CMCC adapter with two physical interfaces, the read and write CMPC or CMPC+ subchannels may be configured on separate physical interfaces.

The **no cmPC** command deactivates the CMPC or CMPC+ subchannel. If the TG is used for a non-High-Performance Routing (HPR) connection, all sessions using the TG will be terminated immediately. If the TG is an HPR connection, all sessions using the TG will be terminated if no other HPR connection is available to the host.

Examples

The following example configures a read and a write subchannel on path C020 for the CMPC or CMPC+ TG named CONFIGE:

```
cmPC C020 F8 CONFIGE READ
cmPC C020 F9 CONFIGE WRITE
```

Related Commands

Command	Description
tg (CMPC)	Defines LLC connection parameters for the CMPC transmission group.
tg (CMPC+)	Defines IP connection parameters for the CMPC+ transmission group.
show extended channel cmPC	Displays information about each CMPC or CMPC+ subchannel configured on the specified channel interface.
show extended channel tg	Displays configuration, operational information, and statistics information for CMPC or CMPC+ transmission groups configured on the virtual interface of the specified CMCC adapter.
show extended channel subchannel	Displays information about the CMCC adapter physical interfaces and displays information that is specific to the interface channel connection. The information displayed generally is useful only for diagnostic tasks performed by technical support personnel.
show extended channel statistics	Displays statistical information about subchannels on the physical interface of a CMCC adapter and displays information that is specific to the interface channel devices. The information generally is useful only for diagnostic tasks performed by technical support personnel.

csna

To configure Systems Network Architecture (SNA) support on a Cisco Mainframe Channel Connection (CMCC) physical channel interface, use the **csna** command in interface configuration mode. This command is used to specify the path and device or subchannel on a physical channel of the router to communicate with an attached mainframe. To delete the Cisco Systems Network Architecture (CSNA) device path, use the **no** form of this command.

```
csna path device [maxpiu value] [time-delay value] [length-delay value]
```

```
no csna path device
```

Syntax Description

<i>path</i>	Hexadecimal value in the range from 0000 to FFFF. This value specifies the logical channel path and consists of two digits for the physical connection (either on the host or on the ESCON director), one digit for the channel logical address, and one digit for the control unit logical address. If the path is not specified in the input/output configuration program input/output configuration program (IOCP), the default value for channel logical address and control unit logical address is 0.
<i>device</i>	Hexadecimal value in the range from 00 to FF. This is the unit address associated with the control unit number and path as specified in the host IOCP file.
maxpiu value	(Optional) Maximum channel I/O block size in bytes that is sent across the physical channel from the CMCC adapter to the attached mainframe. The range is from 4096 to 65535 bytes. The default is 20470 bytes.
time-delay value	(Optional) Number of milliseconds (ms) a host-bound SNA frame may be delayed in order to maximize the channel I/O block size. The range is from 0 to 100 ms. The default is 10 ms.
length-delay value	(Optional) Amount of SNA frame data in bytes the Cisco Systems Network Architecture (CSNA) subchannel accumulates before sending the accumulated channel I/O block to the attached mainframe. The range is from 0 to 65535 bytes. The default is 20470 bytes.

Defaults

maxpiu value: 20470 bytes

time-delay value: 10 ms

length-delay value: 20470 bytes

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

The **maxpiu**, **time-delay** and **length-delay** keywords control the characteristics of host-bound traffic for the CSNA subchannel. The channel protocol used by CSNA allows multiple SNA frames to be blocked into one channel I/O block, reducing the channel bandwidth utilization and mainframe and CMCC adapter process utilization.

The **maxpiu** keyword allows you to set the maximum size of a host-bound channel I/O block.

The **time-delay** keyword instructs the CSNA subchannel to delay sending the channel I/O block for the specified time in milliseconds, from the time the first SNA packet is blocked. This can increase the network latency for an SNA packet by up to the specified time delay.

The **length-delay** keyword instructs the CSNA subchannel to delay sending the channel I/O block until it contains the number of bytes specified by the **length-delay** keyword. An accumulated block is sent to the mainframe if one of the following conditions is true:

- **Time delay** expires
- Channel I/O block reaches the **length-delay** size
- Channel I/O block reaches the **maxpiu** size.

A time delay value of 0 instructs the CSNA subchannel to send SNA packets to the mainframe as soon as they are received from the network. A length delay value of 0 instructs the CSNA subchannel to ignore this parameter.

The **no csna** command deactivates and removes the CSNA subchannel configuration. It also deactivates all Logical Link Control, type 2 (LLC2) sessions established over the subchannel.

Examples

The following example shows CSNA, offload, and Common Link Access for Workstations (CLAW) configured on a channel interface. CSNA has no dependencies to CLAW, offload, or CMPC.

```
interface channel 1/0
no ip address
no keepalive
offload c700 c0 172.18.1.127 TCPIP OS2TCP TCPIP TCPIP TCPIP API
claw C700 c2 172.18.1.219 EVAL CISCOVM AAA BBB
csna c700 c4
csna c700 c5 maxpiu 65535 time-delay 100 length-delay 65535
csna c700 c6 maxpiu 65535 time-delay 100
```

Related Commands

Command	Description
adapter	Configures internal adapters.
lan	Configures an internal LAN on a CMCC adapter interface and enters the internal LAN configuration mode.
show extended channel connection-map llc2	Displays the number of active LLC2 connections for each SAP and the mapping of the internal MAC adapter and the SAP to the resource that activated the SAP.
show extended channel csna	Displays information about the CSNA subchannels configured on the specified CMCC interface.

Command	Description
show extended channel statistics	Displays statistical information about subchannels on the physical interface of a CMCC adapter and displays information that is specific to the interface channel devices. The information generally is useful only for diagnostic tasks performed by technical support personnel.
show extended channel subchannel	Displays information about the CMCC adapter physical interfaces and displays information that is specific to the interface channel connection. The information displayed generally is useful only for diagnostic tasks performed by technical support personnel.

dbconn license

To configure client licenses for Cisco Transaction Connection (CTRC) connections to DATA BASE2 (DB2) or Customer Information Control System (CICS), use the **dbconn license** command in global configuration mode. To remove the licenses, use the **no** form of this command in privileged EXEC configuration mode.

```
dbconn license license-key [connections licensed-connections] [expiration-date yyyymmdd]
```

```
no dbconn license
```

Syntax Description		
	<i>license-key</i>	License key obtained from your Cisco representative. The license key is a 32-character hexadecimal string that specifies the maximum number of CICS conversations or DB2 connections allowed for the CTRC router. The license key is generated for a specific router, and is based on the Systems Network Architecture (SNA) Switching Services control point name (CpName) for the router. Use the show config include cpname command to display the cpname so that you can provide it when you request the license key.
	connections <i>licensed-connections</i>	Number of licensed connections. If the license is for an unlimited number of connections, omit the connections keyword.
	expiration-date <i>yyyymmdd</i>	Date when a temporary license key expires, where <i>yyyy</i> is the year expressed in four digits, <i>mm</i> is the month expressed in two digits, and <i>dd</i> is the date expressed in two digits. If the license is for an unlimited time period (permanent license), omit the expiration-date keyword.

Defaults If the number of licensed connections is not specified, the license key must allow an unlimited number of licensed connections. If the expiration date is not specified, the license key must be for a permanent license.

Command Modes Global configuration

Command History	Release	Modification
	11.3(2)T	This command was introduced.
	12.0(5)XN	This command was moved from the Cisco Database Connection (CDBC) feature to the CTRC feature.
	12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines Licenses are required for all CTRC installations. For testing and evaluation purposes, unlicensed CTRC installations allow you to establish two connections to DB2, or two conversations to CICS, or one to each. One license key is used for both CICS and DB2 communications, so you can use either the **dbconn license** command or the **txconn license** command to configure the CTRC router.

Examples

The following example shows the configuration of a CTRC router with a license that allows up to 4000 connections until January 1, 2005:

```
dbconn license 3C09A051320BAF020BFF45B3A2FF21D2 connections 4000 expiration-date 20050101
```

Related Commands

Command	Description
show dbconn license	Displays the status of CTRC licenses for DB2 communications.
show snasw node	Displays details and statistics of the SNASw operation.
show txconn license	Displays the status of licenses used for CTRC.
txconn license	Licenses a Cisco router for CTRC communications with CICS or DB2.

dbconn pem

To configure password expiration management (PEM) support for connections to DATABASE2 (DB2), use the **dbconn pem** command in global configuration mode. To remove PEM support, use the **no** form of this command.

```
dbconn pem server server-name rlu rlu-name mode mode-name [tpname tp-name]
```

```
no dbconn pem server server-name
```

Syntax Description

server <i>server-name</i>	Name of the Cisco Transaction Connection (CTRC) server that you want to configure for password management.
rlu <i>rlu-name</i>	Host remote logical unit (LU) name the server connects to when performing password management. This remote logical unit (RLU) ordinarily differs from the RLU values used in dbconn server or txconn destination commands. It may or may not be fully qualified.
mode <i>mode-name</i>	APPC stack mode the server uses when performing password management.
tpname <i>tp-name</i>	(Optional) Name of the PEM transaction program on the host (the APPC Signon transaction program, a designed Advanced Program-to-Program Communication (APPC) termination point (TP). The default value is \x06301 (0x06F3F0F1 in EBCDIC).

Defaults

If the *tp-name* assignment is not specified, the default value is \x06301 (0x06F3F0F1 in EBCDIC).

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.

Examples

The following example shows the configuration of PEM support on a CTRC server named DB2BUDD:

```
dbconn pem DB2BUDD rlu MVSLU01 mode #INTER
```

Related Commands

Command	Description
show dbconn server	Displays information about CTRC servers configured for DB2 communications.

dbconn ping

To determine whether Cisco Transaction Connection (CTRC) servers are connecting to DATABASE2 (DB2) host databases, use the **dbconn ping** command in user EXEC or privileged EXEC mode.

dbconn ping *server-name* [**userid** *user-id*] [**password** *password*] [**rdbname** *rdbname*]

Syntax Description

<i>server-name</i>	Name of the CTRC server for DB2 communications.
userid <i>user-id</i>	(Optional) User ID used to connect to the DB2 system.
password <i>password</i>	(Optional) Password used to connect to the DB2 system.
rdbname <i>rdbname</i>	(Optional) Name of the relational database to be contacted.

Defaults

If no user ID is specified, the ping connection is made without Advanced Program-to-Program Communication (APPC) security. The DB2 system's security settings determine whether the ping can succeed.

If no *rdbname* value is specified, the relational database name configured for the CTRC server is used.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.3(2)T	This command was introduced.
12.0(5)XN	This command was moved from the Cisco Database Connection (CDBC) feature to the CTRC feature.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.

Usage Guidelines

This command can be used for CTRC servers that communicate with DB2 over either Systems Network Architecture (SNA) or TCP/IP (dbconn servers and dbconn tcpservers). There is not a **no** form this command.

Examples

The following example illustrates using the **dbconn ping** command to verify the connection to the default database for the CTRC server SERVER-1:

```
dbconn ping SERVER-1
```

```
RDB named DB2510 on database server SERVER-1 successfully contacted!
Database server product id is QSQ03020, DB2 for OS/400 V3R2
Elapsed time was 00:00:00
```

Related Commands

Command	Description
ping sna	Initiates an APPC session with a named destination LU to run the APING transaction program to check network integrity and timing characteristics.
show dSystems Network Architecture (SNA)bconn server	Displays information about CTRC servers configured for DB2 communications.

dbconn server

To configure a Cisco Transaction Connection (CTRC) server process for Advanced Program-to-Program Communication (APPC) communications with DATABASE2 (DB2), use the **dbconn server** command in global configuration mode. To disable the server and remove its configuration, use the **no** form of this command.

```
dbconn server server-name [idle-timeout minutes] [ipaddress ip-address] [keepalive attempts
number] [keepalive interval seconds] [mode mode] [port port-number] [rdbname rdbname]
[rlu remote-lu] [tpname tp-name] [window-size bytes] [wlm {off | on}]
```

```
no dbconn server server-name
```

Syntax	Description
server-name <i>server-name</i>	Name of the CTRC server. Server names are user-defined strings up to 16 characters in length.
idle-timeout <i>idle-timeout</i>	(Optional) Time, in minutes, to wait for an idle client. If there is no activity from the client for this amount of time, the connection is forcibly broken. The time spent in waiting for a response from the DB2 system is not counted; only idle time in between client requests is counted. The maximum is 1440 minutes (24 hours). If no idle timeout is specified, the default is 0 (zero) for no timeout.
ipaddress <i>ip-address</i>	(Optional) IP address used by the CTRC server to receive a connection requesting DB2 communications. When a connection arrives, this IP address is used for matching and selecting the server from multiple configured servers. If you do not specify an IP address, the current server can handle DB2 connectivity requests sent to any IP address on the local router.
keepalive attempts <i>number</i>	(Optional) The number of times for the CTRC server to attempt sending an acknowledgment message to the client to keep the connection alive. You can specify 1 to 100 attempts, or 0 (zero) to disable the keepalive messages. The default is 3 attempts.
keepalive interval <i>seconds</i>	(Optional) The frequency for the CTRC server to send an acknowledgment message to the client to keep the connection alive. The interval can be from 1 to 3600 seconds, or 0 (zero) to disable the keepalive messages. The default is 120 seconds.
mode <i>mode</i>	(Optional) APPC mode used to allocate the conversation to the DB2 system. If no mode is specified, the default is #INTER. Performance might improve if you choose a mode such as IBMRDB. If you specify a mode that does not already exist, CTRC will create it.
port <i>port-number</i>	(Optional) Port used to listen for connections requesting DB2 communications. If no port is specified, the default is 446.
rdbname <i>rdbname</i>	(Optional) DB2 remote database name on the host. When a connection arrives, this name is used to identify and select the appropriate server from multiple configured servers. The string is used to match the relational database (RDB) name sent by the client in the Distributed Relational Database Architecture (DRDA) data stream at connect time. The default relational database (RDB) name is an asterisk (*), which indicates that this CTRC server serves any remote database.

rlu <i>remote-lu</i>	(Optional) APPC remote logical unit (LU) used to allocate the connection to the DB2 system. An example is NETA.S103B345. If no remote LU is specified, the default is the configured server name that is set to uppercase and truncated to eight characters. An RLU need not be qualified with a NET ID. If you omit the network entity title (NET) ID, the NET ID of the router's Systems Network Architecture (SNA) Switching Services control point is used to fully qualify the LU name.
tpname <i>tp-name</i>	(Optional) APPC remote transaction program name used to allocate the conversation to the DB2 system. If no termination point (TP) name is specified, the default is the designed DRDA TP name \x076DB.
window-size <i>bytes</i>	(Optional) TCP/IP receive window size. The maximum window size you can specify is 65535 bytes, and the default is 4096 bytes.
wlm { off on }	(Optional) Enables or disables Workload Manager load balancing. The default is "inactive-enabled."

Defaults

If you do not specify an idle timeout, client connections can continue regardless of how long they have been idle.

If you do not specify an IP address, the current server can handle DB2 connectivity requests sent to any IP address on the local router.

If you do not specify a keepalive attempt or a keepalive interval, the server makes up to three attempts to send an acknowledgment message every 120 seconds.

If you do not specify an APPC mode, the default value is #INTER. If you specify a mode that does not already exist, CTRC will create it.

If you do not specify a port number, the current server uses the default value of 446.

If you do not specify an RDB name, the server is configured to serve any remote database.

If you do not specify a remote LU, the default is the configured server name that is set to uppercase and truncated to eight characters. An RLU need not be qualified with a NET ID. If you omit the NET ID, the NET ID of the router's SNA Switching Services control point is used to fully qualify the LU name.

If you do not specify an APPC transaction program name, the default value is the designed DRDA TP name \x076DB.

If you do not specify a TCP receive window size, the default value is 4096 bytes.

The Workload Manager load balancing default is "inactive-enabled."

Command Modes

Global configuration

Command History

Release	Modification
11.3(2)T	This command was introduced.
12.0(5)XN	This command was moved from the CDBC feature to the CTRC feature.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.
12.1(5)T	This command was enhanced to allow configuration of keepalive messages.

Usage Guidelines

You can configure more than one CTRC server per router for communications with DB2 or Customer Information Control System (CICS). There is no limit on the number of CTRC servers. For each DB2 database system in your network, you can configure a CTRC server in the router configuration. Servers that are configured on the same router can share a port. CTRC txconn servers should use a different port. Set the **keepalive attempts** or **keepalive interval** keyword to zero (0) to disable the keepalive messages.

Examples

The following example shows configuring a CTRC server named SERVER-1 to manage communications to a DB2 database named DB2510, using the IBMRDB APPC mode to allocate the conversation, and attempting five acknowledgment messages every 300 seconds:

```
dbconn server SERVER-1 idle-timeout 20 keepalive attempts 5 keepalive interval 300 mode
IBMRDB rdbname DB2510 rlu STARW.SERVER-1
```

Related Commands

Command	Description
clear dbconn connection	Breaks a client connection to DB2.
dbconn ping	Determines whether or not CTRC servers are successfully connecting to DB2 host databases.
show dbconn ports	Displays information about ports used for CTRC server communications to DB2.
show dbconn server	Displays information about CTRC servers configured for DB2 communications.
show snasw mode	Displays information about SNASw modes.

dbconn tcpserver

To configure a Cisco Transaction Connection (CTRC) server process to communicate with IP-enabled DATABASE2 (DB2) databases, use the **dbconn tcpserver** command in global configuration mode. To disable a server and remove its configuration, use the **no** form of this command.

```
dbconn tcpserver server-name [idle-timeout minutes] [ip ip-address] [keepalive attempts
number] [keepalive interval seconds] [port port-num] [rdbname rdbname]
[remote-hostname remote-hostname | remote-ip remote-ip-address] [remote-keepalive
attempts number] [remote-keepalive interval seconds] [remote-port remote-port]
[window-size bytes] [wlm {off | on}]
```

```
no dbconn tcpserver server-name
```

Syntax Description

<i>server-name</i>	Name of the CTRC server being configured for TCP pass-through communications with DB2.
idle-timeout <i>minutes</i>	(Optional) Time, in minutes, to wait for an idle client. If there is no activity from the client for this amount of time, the connection is forcibly broken. The time spent in waiting for a response from the DB2 system is not counted; only idle time in between client requests is counted. The maximum time is 1440 minutes (24 hours). If no idle timeout is specified, the default is 0 (zero) for no timeout.
ip <i>ip-address</i>	(Optional) IP address for the CTRC tcpserver process being configured. If not specified, the tcpserver receives client requests on all IP addresses configured for the router.
keepalive attempts <i>number</i>	(Optional) The number of times for the CTRC server to attempt sending an acknowledgment message to the client to keep the connection alive. You can specify 1 to 100 attempts, or 0 (zero) to disable the keepalive messages. The default is three attempts.
keepalive interval <i>seconds</i>	(Optional) The frequency for the CTRC server to send an acknowledgment message to the client to keep the connection alive. The interval can be from 1 to 3600 seconds, or 0 (zero) to disable the keepalive messages. The default is 120 seconds.
port <i>port-num</i>	(Optional) Port the tcpserver listens on for client requests. The default value is 446. A dbconn server and a dbconn tcpserver can share the same port.
rdbname <i>rdbname</i>	(Optional) DB2 remote database name on the host. When a connection arrives, this name is used to identify and select the appropriate tcpserver from multiple configured tcpserver. The string is used to match the relational database (RDB) name sent by the client in the DRDA data stream at connect time. The default RDB name is an asterisk (*), which indicates that this CTRC tcpserver serves any remote database.
remote-hostname <i>remote-hostname</i> remote-ip <i>remote-ip-address</i>	DNS host name of the remote database server to which you want to connect, or the IP address for the host where DB2 resides. You must specify either the name or the IP address of the host.

remote-keepalive attempts <i>number</i>	(Optional) The number of times for the CTRC server to attempt sending an acknowledgment message to the host to keep the connection alive. You can specify 1 to 100 attempts, or 0 (zero) to disable the keepalive messages. The default is three attempts.
remote-keepalive interval <i>seconds</i>	(Optional) The frequency for the CTRC server to send an acknowledgment message to the host to keep the connection alive. The interval can be from 1 to 3600 seconds, or 0 (zero) to disable the keepalive messages. The default is 120 seconds.
remote-port <i>remote-port</i>	(Optional) Host port that listens for tcpserver communications from the router. The default value is 446.
window-size <i>bytes</i>	(Optional) This value is used for the TCP/IP receive window size. If no window size is specified, the default is 4096 bytes.
wlm {off on}	(Optional) Enables or disables Workload Manager load balancing. The default is "inactive-enabled."

Defaults

If you do not specify an idle timeout period, the default value is zero for no timeout.

If you do not specify an IP address for the tcpserver, it can receive requests on any IP address configured for the router.

If you do not specify a keepalive attempt or a keepalive interval, the server makes three attempts to send an acknowledgment message to the client every 120 seconds. If you do not specify a remote keepalive attempt or a remote keepalive interval, the server makes three attempts to send an acknowledgment message to the host every 120 seconds.

If you do not specify a port for the tcpserver, the default port is 446.

If you do not specify a remote database name for the DB2 system, the tcpserver can communicate with any RDB name.

If you do not specify a port for the remote DB2 system, the tcpserver uses the default value of 446.

If you do not specify a TCP/IP receive window size, the default value is 4096 bytes.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.
12.1(5)T	This command was enhanced to allow configuration of the keepalive interval.

Usage Guidelines

Configure a separate tcpserver for each DB2 system IP address. A dbconn server and a dbconn tcpserver can share the same port.

Examples

The following example shows configuring a tcpserver named BUDDTCP to manage connections to a DB2 database named DB2510, attempting up to five keepalive messages to the client and to the host every 300 seconds:

```
dbconn tcpserver BUDDTCP keepalive attempts 5 keepalive interval 300 port 446 rdbname
DB2510 remote-ip 198.147.235.39 remote-keepalive attempts 5 remote-keepalive interval 300
remote-port 446
```

Related Commands

Command	Description
dbconn ping	Determines whether or not CTRC servers are successfully connecting to DB2 host databases.
show dbconn server	Displays information about CTRC servers configured for DB2 communications.

default-profile

To specify the name of the profile to be applied as a default to all the listen points, use the **default-profile** command in security configuration mode. To disable the default profile specification, use the **no** form of this command.

default-profile *profilename*

no default-profile *profilename*

Syntax Description	<i>profilename</i>	A profile name that has already been configured.
---------------------------	--------------------	--

Defaults	No default profile.
-----------------	---------------------

Command Modes	Security configuration
----------------------	------------------------

Command History	Release	Modification
	12.1(5)T	This command was introduced.

Usage Guidelines	<p>If this command is configured, this profile name and all of its attributes will be associated with all listen points that do not specify an individual profile with the sec-profile command.</p>
-------------------------	--

Profile names cannot be duplicated.

Entering the **no** form of this command removes the default specification and any listen points that do not have the **sec-profile** command specified will revert to a nonsecure mode.

This command has no retroactive effect. If a listen point is specified using the **listen-point** command, and the **sec-profile** command was already configured for that listen point, then all client connections to that listen point will be secure.

If a listen point is specified using the listen-point command, and the **default-profile** command is not configured, then all client connections to that listen point will not be secure. However, if the **default-profile** command is later configured, then all now connections to that listen point will be secure using the specified **default-profile** command. This will not affect the nonsecure connections.

Examples	<p>The following example specifies DOMESTIC as the default profile name for all clients connecting to listen point 10.10.10.1 until the default-profile LAM command is configured. Once the default-profile LAM command is configured, all new client connections will use LAM as the default profile.</p>
-----------------	--

```
tn3270
 security
  profile NOSECURITY none
  default-profile DOMESTIC
pu DIRECT 012ABCDE tok 0 04
  default-profile LAM
listen-point 10.10.10.1
```

Related Commands

Command	Description
profile	Specifies a name and a security protocol for a security profile and enters profile configuration mode.
sec-profile	Specifies the security profile to be associated with a listen point.

disable (TN3270)

To turn off security in the TN3270 server, use the **disable** (TN3270) command in security configuration mode.

disable

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Security configuration

Command History	Release	Modification
	12.1(5)T	This command was introduced.

Usage Guidelines Configuring the **disable** command does not terminate any active secure or nonsecure connections. This command specifies that all new connections established with the TN3270 server will be nonsecure. If a client initiates a change cipher specification for an existing secure connection, then the TN3270 server will process the request.

There is not a **no** form for this command. The **enable** command is equivalent to the **no** form of this command.

Examples The following example turns off security in the TN3270 server so that all new connections established with the TN3270 server will be nonsecure:

```
disable
```

Related Commands	Command	Description
	enable (TN3270)	Turns on security in the TN3270 server.